

# Impossibile caricare l'interfaccia utente di CCM dopo un aggiornamento

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Problema: Impossibile caricare l'interfaccia utente di CCM dopo un aggiornamento](#)

[Soluzione](#)

## Introduzione

Questo documento descrive come risolvere un problema in cui l'interfaccia utente di Cisco Call Manager (CCM) non viene caricata dopo un aggiornamento,

## Prerequisiti

### Requisiti

Nessun requisito specifico previsto per questo documento.

## Componenti usati

Le informazioni di questo documento si basano sulle versioni da CloudCenter 4.8.1.2 a v4.8.2.1

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Problema: Impossibile caricare l'interfaccia utente di CCM dopo un aggiornamento

Dopo l'aggiornamento di CCM, l'interfaccia utente non viene caricata e in v4.8.2+ viene visualizzata solo una schermata grigia.

Nel file `/usr/local/cliqr/logs/managementserver.log` viene visualizzato questo messaggio di errore:

```
VENDOR_ID:::USER_ID:::2018-03-09 12:54:06,368 ERROR bootstrap.CryptoTextEncryptor [main] -  
Fail to decrypt: cliqr  
VENDOR_ID:::USER_ID:::2018-03-09 12:54:06,382 ERROR boot.SpringApplication [main] -  
Application startup failed  
java.lang.IllegalStateException: Cannot decrypt: key=DATABASE_POSTGRES_PASSWORD
```

# Soluzione

Durante l'aggiornamento, la password utilizzata da CloudCenter per accedere al database postgres è danneggiata. È possibile risolvere il problema durante l'installazione guidata di CCM (se in HA eseguito su entrambi i dispositivi CCM) e reimmettere la password postgres.

```
./usr/local/cliqr/bin/ccm_config_wizard.sh
```

Passare alla scheda Parametri DB e immettere nuovamente la password DB.

Se non si conosce la password DB, contattare Cisco TAC per ottenere la password predefinita, quindi modificarla immediatamente.